

REMARKS

I. Rejection of Claims 1-5, 8-13, 17, 19, and 21 Under 35 U.S.C. § 103

The Office Action rejected Claims 1-5, 8-13, 17, 19, and 21 under 35 U.S.C. § 103(a) as being unpatentable over Sasmazel, in view of Blaze, Roberts, and in further view of Misra. The Office Action asserts that Sasmazel, Blaze, Roberts, and Misra suggest each and every element of Claims 1-5, 8-13, 17, 19, and 21 and that it would be obvious to combine their teachings. Applicant respectfully disagrees.

A. Claim 1

Claim 1 recites:

1. A method for authorizing a client computer to access a second server-based application based upon previously provided authorization to access a first server-based application, comprising:

(a) receiving a request to access said second computer server-based application;

(b) in response to said request:

(i) determining a session length indicating a length of time said client computer has been authorized to access said first server-based application;

(ii) calculating a hash value for an authorization ticket received from said first server-based application, said session length, and a secret shared between said client computer and said second server-based application, and

(iii) transmitting a request for authorization to said second server-based application comprising said hash value, said authorization ticket, and said session length.

As distinctly recited in Claim 1, applicant's invention includes a method for authorizing a client computer to access a first server-based application. Once the client computer is authorized to access the first server-based application, a request to access a second server-based application is also authorized without requiring any additional effort on the part of the user. A user

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PLLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

associated with the client computer does not have to endure a second log-in procedure when making a request to access the second server-based application. Conversely, Sasmazel is directed to a system that allows Web server computers that collectively execute a Web server application to satisfy requests without requiring user authorization when requests are handled by a single application.

The Office Action asserts that Sasmezel discloses:

[a]n eticket architecture generated by an authentication server that may then be transmitted over the Internet from server to server (i.e. server-based application) without having the information in the eticket altered, and without having to authenticate the user at each server (multiple server-based application is inherent).

(Office Action at p. 2.)

The Office Action incorrectly equates a server computer with a server-based application and states that authentication to multiple server-based applications is inherent, even though not explicitly disclosed, in Sasmazel. However, authentication to multiple server-based applications is not inherent in the teachings of Sasmazel. Instead, the eticket architecture as described in Sasmazel is limited to authenticating a user at a single server-based application program, the functions of which may be distributed over multiple computers (e.g., Web servers). As stated in Sasmazel, the eticket architecture "will provide a much more confined user and World Wide Web based application system by providing a user session concept with the 'eticket' architecture. **This ticketing architecture will tie the user browser to the Internet Server (or application).**" (Emphasis added). Sasmazel at Col. 10, lines 40-45. Sasmazel does not disclose a method for authorizing a client computer to access a second server-based application based upon previously provided authorization to access a first server-based application. Instead, Sasmazel discloses a system where authentication is tied to a single application, such as a Web server, the logic and

resources of which may be distributed among multiple computers. This distinction is also evident from Claim 1 in Sasmazel that recites:

receiving a request at a plurality of **web servers**, said request including a service request and said electronic ticket;
determining authorization of said request received **at each of said web servers** by determining authorization of said electronic ticket. . . .
(Emphasis added.)

Sasmazel, Col. 11, lines 3-10.

Simply stated, the present invention authorizes users to access multiple server-based applications (e.g., a Web server application, instant messaging server application, and the like) without having to be re-authenticated when logic or resources from another server-based application is needed. For example, a user of the present invention may open an account from a single provider that offers multiple services. In this regard, the user may attempt to access a restricted Web page from a Web server associated with the provider that requires authentication. After being authenticated, the user may access the Web page. However, based on the previous authentication, the user may also use an application program, for example, that allows instant messaging with another user. In this regard, a server-based instant messaging application program associated with the provider may obtain the user's authentication rights from the Web server application program. This functionality is described in the present invention as follows:

According to an embodiment of the present invention, a user of the client computer may select a user interface option provided by the instant messaging client application program 12 for gaining quick access to the Web server computer. For instance, a user of the MSN Messenger client application may desire to quickly gain access to their Web-based e-mail account with the HotMail service, also from Microsoft®. In order to provide this functionality, the instant messaging client application program 12 may provide a menu item, button, or other user interface item for quickly accessing the Web server computer 26. In response to the selection of this user interface item, the client computer 10 may gain authorization to access to the Web server computer 26 based upon the

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PLLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

previously provided authorization to access the instant messaging server computer 2. Present application at page 7.

Thus, unlike Sasmazel, the claims recited in present invention are not limited to authorizing a user to access the resources and logic of a specific application. More specifically, Claim 1 of the present invention recites a method for authorizing a client computer to access a second server-based application based upon previously provided authorization to access a first server-based application. The claimed method recites (a) calculating a hash value for an authorization ticket received from **said first server-based application**, and (b) transmitting a request for authorization to **said second server-based application** comprising said hash value, said authorization ticket, and said session length.

The Office Action admits that Sasmazel does not specifically disclose "determining a session length indicating a length of time the client computer has been authorized to access said first server-based application." However, the Office Action asserts that Blaze discloses determining a session length indicating a length of time the user is authorized to access a server-based application. Applicant respectfully disagrees. In support of that proposition, the Office Action states:

Blaze teaches that once a smart card (i.e. the client) is deemed valid (i.e. a session is started), the smart card may be used to decrypt one or more files stored in the system. The smart card uses a clock to start a timer, ascertain the data in time at which the file decryption occurred, and store such time and date in appropriate fields. The smart card stores in a field of activity storage area the length of time during which the **escrow agent had access to the encrypted filesystem**. (Emphasis added).

In addition to the reasoning provided in response to the previous Office Action, Blaze does not disclose "indicating a length of time the client computer has been authorized to access said **first server-based application**." (Emphasis added.) Instead, as noted in the Office Action, Blaze discloses a system in which a "smartcard stores in a field of activity storage area the length of time during which the escrow agent had access to the encrypted filesystem." Providing access

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PLLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

to server-based applications as disclosed in the present invention is not the same as providing access to an encrypted filesystem as disclosed in Blaze. Among other things, server-based applications may provide logic (e.g. processing) and resources to a user. By contrast, a filesystem may only be used to access data.

For at least the above-mentioned reasons, applicant respectfully submits that the Office Action has not established a *prima facie* case for a Section 103(a) rejection of Claim 1, and respectfully requests that the rejection of Claim 1 and the claims dependent thereon be withdrawn and these claims allowed.

B. Claim 13

Claim 13 recites:

13. A method for authorizing a client computer to access a second server-based application based upon previously provided authorization to access a first server-based application, comprising:

(a) receiving a request for authorization to access said second server-based application from said client computer comprising a hash value, an authorization ticket, and a session length;

(b) computing a new hash value for said authorization ticket, said session length, and a copy of a secret shared between said client computer and said second server-based application;

(c) determining whether said hash value received from said client computer is identical to said new hash value; and

(d) in response to determining that said hash value received from said client computer is identical to said new hash value, authorizing said client computer to access said second server-based application.

Claim 13 of the present invention recites a method for authorizing a client computer to access a second server-based application based upon previously provided authorization to access a first server-based application. More specifically, the claimed method recites (a) receiving a request for authorization to access said second server-based application from said client computer comprising a hash value, an authorization ticket, and a session length, (b) computing a

new hash value for said authorization ticket, said session length and a copy of a secret shared between said client computer and said second server-based application, and (c) in response to determining that said hash value received from said client computer is identical to said new hash value, authorizing said client computer to access said second server-based application.

As described previously with regard to Claim 1, Sasmazel does not disclose a method for authorizing a client computer to access a second server-based application based upon previously provided authorization to access a first server-based application. Instead, Sasmazel purportedly discloses a system where authentication is tied to a single application, such as a Web server application, that may be distributed among multiple computers. Conversely, the present invention authenticates users to access multiple server-based applications. Thus, the present invention is not limited to authorizing a user to access a specific application. Consequently, Sasmazel does not disclose the elements as recited in Claim 13, and applicant respectfully submits that the rejection of Claim 13 is in error and requests that the rejection be withdrawn.

The Office Action admits that Sasmazel does not specifically disclose "including a session length in the request for authorization." However, the Office Action asserts that Roberts discloses including a session length in the request for authorization. Applicant respectfully disagrees.

Roberts purportedly discloses a system for automatically collecting customer profile information when a customer accesses a company Web site. After the customer profile information is known, dynamic content is selected and displayed in accordance with the profile information. The Roberts system for gathering customer profile information includes logging a customer's passive activity (i.e., time spent viewing a particular Web page). The Office inferred that the time spent viewing a particular Web page is substantially similar to a session length. Office Action at page 7. However, logging a customer's passive activity is not the same as

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PLLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

"including a session length in the request for authorization." In fact, Roberts does not involve authenticating users to access any Web content. Instead, Roberts is only concerned with monitoring customers and providing customized Web pages and does not disclose including "a session length in a request for authorization." Simply stated, in the Roberts system the client computer does not make a request for authorization as it is only concerned with monitoring the activities of the user.

For at least the above-mentioned reasons, applicant respectfully submits that the Office Action has not established a *prima facie* case for a Section 103(a) rejection of Claim 13 and respectfully requests that the rejection of Claim 13 and the claims dependent thereon be withdrawn.

C. Claims 2-5, 8-12, 17, 19, and 21

Since Claims 2-5 and 8 depend, directly or indirectly, from Claim 1 and Claims 9-10 and 11-12 are computer apparatus and computer-readable medium claims that depend from Claims 1 and 2. Thus, the analysis applied to Claim 1 also applies to these claims. Also, since Claim 21 depends from Claim 13 and Claims 17 and 19 are computer-controlled apparatus and computer-readable medium claims that depend from Claim 13, the analysis applied to Claim 13 also applies to these claims. Therefore, applicant respectfully submits that Claims 2-5, 8-12, 17, 19, and 21 are in condition for allowance for the same reasons as Claims 1 and 13, respectively. In addition, applicant submits that the dependent claims are allowable for additional reasons described below.

Claim 2 recites a combination of steps "wherein said authorization ticket comprises a time stamp, and wherein determining a session length comprises subtracting said time stamp from an elapsed time counter to determine said session length." Applicant was previously unable to find any reference in Misra to a time counter or any other mechanism for determining a

session length. The Office Action states that "Misra teaches that the timestamp helps to minimize the time period in which an eavesdropper may use a copied ticket (which includes a session key) and authentication pair. This suggests a time counter for determining session length based on a value of an elapsed time counter." Office Action at page 3. Applicant submits that the Office Action uses hindsight to read items into the teaching of Misra that does not exist. Simply stated, the claimed combination of determining a session length based on the value of an elapsed time counter is not well known in the art and not disclosed or suggested in Misra. Therefore, applicant respectfully submits that Claim 2 is also in condition for allowance for these additional reasons.

Dependent Claims 3-4 add to the nonobviousness of applicant's invention of starting the elapsed time counter "when said authorization ticket is received from said first server-based application." Applicant submits that Blaze only stores data related to the use of a smartcard. Storing time and date information related to the use of a smartcard is not the same as determining when to start an elapsed time counter. Therefore, applicant respectfully submits that Claims 3 and 4 are also in condition for allowance for these additional reasons.

Dependent Claim 5 adds to the nonobviousness of applicant's invention of "performing an MD5 hash of an authorization ticket received from said first server-based application, said session length, and a secret shared between said client computer and said second server-based application." The Office Action asserts that Sasmazel teaches performing an MD5 hash of an authorization ticket that includes a session length and a shared secret, and references Col. 2, lines 41-42, of Sasmazel in support of that proposition. The referenced section of Sasmazel states that an MD5 protocol is used to "hash the information in the data packet." However, Sasmazel indicates that the data packet only includes "authorization information." Sasmazel at Col. 2, lines 32-33. The present invention provides a more secure environment by hashing data

in addition to authentication information. More specifically, Claim 5 recites "performing an MD5 hash of an authorization ticket that includes a session length and a secret." Obviously, a session length stored on a client computer is not the same as authentication information. Therefore, applicant respectfully submits that Claim 5 is also in condition for allowance for these additional reasons.

Dependent Claims 8 and 21 add to the nonobviousness of applicant's invention by specifying that the first server-based application is an instant messaging server and specifying that the second server-based application is a Web server. The Office Action asserts that Sasmazel teaches "that the first computer comprises an instant messaging server computer (i.e., Web server) and that the second computer comprises a Web server computer." Office Action at page 6. The Office Action equates an instant messaging server with a Web server. However, an instant messaging server is not equivalent to a Web server. As known to those skilled in the art and others, an instant messaging server is used to establish "chat" sessions between client computers connected to a network. Conversely, a Web server transmits files such as hypertext documents between a server computer and a client computer. Therefore, applicant respectfully submits that Claims 8 and 21 are also in condition for allowance for these additional reasons.

II. Rejection of Claims 6-7 Under 35 U.S.C. § 103

The Office Action rejected Claims 6-7 under 35 U.S.C. § 103(a) as being unpatentable over Sasmazel, in view of Blaze, Roberts, and Misra, as applied to Claim 1 and further in view of Wang. The Office Action asserts that Sasmazel, Blaze, Roberts, Misra, and Wang suggest each and every element of Claims 6-7 and that it would be obvious to combine their teachings. Applicant respectfully disagrees. Since Claims 6-7 depend from Claim 1, the analysis applied to Claim 1 also applies to these claims. In addition, applicant submits that these dependent claims are allowable for additional reasons described below.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PLLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

Dependent Claim 6 adds to the nonobviousness of applicant's invention the combination of (1) starting a persistence timer; (2) determining whether said persistence timer has reached a predefined value prior to receiving a response from said server-based application; and (3) in response to determining that said persistence timer has reached a predefined value prior to receiving a response from said second server-based application, deleting said authorization ticket, said session length and said hash value from said client computer." The Office Action asserts that Wang teaches these additional elements recited in Claim 6, stating that "Wang teaches that when a data packet (i.e., authentication ticket) is sent, a sequence variable is allocated and an acknowledgement timer (i.e., persistence timer) is set to prevent waiting indefinitely." Office Action at page 9. However, a system that prevents deadlocks (i.e., waiting indefinitely) as disclosed in Wang is not equivalent to the elements recited in Claim 6. More specifically, Claim 6 recites using a persistence timer to periodically check to determine if a predetermined amount of time has elapsed. This is not equivalent to using an acknowledgement timer to prevent deadlocks. Therefore, applicant respectfully submits that Claim 6 is also in condition for allowance for these additional reasons.

Dependent Claim 7 adds to the nonobviousness of applicant's invention the combination of "in response to determining that said persistence timer has not reached a predefined value prior to receiving a response from said second server-based application, receiving said response from said second server-based application and displaying said response at said client computer." The Office Action asserts that Wang teaches the additional elements recited in Claim 7. However, applicant is unable to find any reference in Wang to displaying the results of an authentication process. Instead, Wang is directed to a channel access protocol for implementing a wireless data network that does not involve interactions with a user. Therefore, applicant respectfully submits that Claim 7 is also in condition for allowance for these additional reasons.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PLLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

III. Rejection of Claims 14-16, 18, and 20 Under 35 U.S.C. § 103

The Office Action rejected Claims 14-16, 18, and 20 under 35 U.S.C. § 103(a) as being unpatentable over Sasmazel, in view of Blaze, Roberts, and Misra as applied to Claim 13 and further in view of Hershey. The Office Action asserts that Sasmazel, Blaze, Roberts, Misra, and Hershey suggest each and every element of Claims 14-16, 18, and 20. Applicant respectfully disagrees.

A. Claims 14-16

Since Claims 14-16 depend from Claim 13, the analysis applied to Claim 13 also applies to these claims. In addition, applicant submits that these dependent claims are allowable for additional reasons described below.

Dependent Claims 14-16 add to the nonobviousness of applicant's invention the combination of

"(1) in response to determining that said hash value received from said client computer is identical to said new hash value, (2) determining whether a sum of said session length and a time stamp received as part of said authorization ticket is within a preset threshold value of a current time, and (3) in response to determining that the sum of said session length and said time stamp is within said preset threshold value, authorizing said client computer to access said second server-based application."

The Office Action asserts that Hershey teaches these additional elements and cites Col. 7, lines 34-43, of Hershey in support of that proposition. Applicant submits that Hershey does not authorize client computers to access any server-based application. Instead, the system disclosed in Hershey determines if "the current message packet has expired" using a time stamp. Hershey at Col. 7, lines 38-40. If the message packet has not expired, then the message is rebroadcast. Applicant submits that rebroadcasting a message packet based on a time stamp is not equivalent to "authorizing said client computer to access said second server-based application." Therefore,

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PLLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

applicant respectfully submits that Claims 14-16 are also in condition for allowance for these additional reasons.

B. Claims 18 and 20

Claims 18 and 20 are directed to computer apparatus and computer-readable mediums having language that depend from Claim 14. Thus the analysis applied to Claim 14 also applies to these claims. Therefore, applicant respectfully submits that Claims 18 and 20 are in condition for allowance for the same reasons as Claim 14.

CONCLUSION

In view of the remarks above, applicant respectfully submits that the present application is in condition for allowance. Reconsideration and reexamination of the application and allowance of the claims at an early date are solicited. If the Examiner has any questions or comments concerning this matter, the Examiner is invited to contact the applicant's undersigned attorney at the number below.

Respectfully submitted,

CHRISTENSEN O'CONNOR
JOHNSON KINDNESS^{PLLC}



Clint J. Feekes
Registration No. 51,670
Direct Dial No. 206.695.1633

I hereby certify that this correspondence is being deposited with the U.S. Postal Service in a sealed envelope as first class mail with postage thereon fully prepaid and addressed to MAIL STOP AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the below date.

Date: July 14, 2005



CJF:mgp

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PLLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100